UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/827,226	04/05/2001	Marcus Wong	1	6211

7590 08/10/2005

David J. Gaskey
Carison, Gaskey & Olds, PC
400 West Maple Road
Suite #350
Birmingham, MI 48009

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/827,226	WONG, MARCUS	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/8/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's arguments/amendments with respect to claims 1-20, filed on **April 14, 2005** have been fully considered but they are not persuasive. The examiner would like to point out that this action is made final (MPEP 706.07a).

Response to Arguments

2. Applicant argues that:

a. Independent claims 1, and 13 are not taught by neither of the references, Johnston, Terao, and Ellison, to include *"a common key that is provided to a first wireless unit and that is used* ***for communication between first and second wireless unit****"(page 6 par. 4 and page 7 par. 1).*

b. Dependent claims 2-12, and 14-20 are allowable based upon their dependency on allowable claims 1 and 13 (page 7 par. 2).

However, Examiner disagrees with applicant.

Regarding argument (a), Argument is not persuasive. Ellison teaches key generator device that generates a symmetric/common key and ciphers the generated common key with another key and transmits the ciphered key to another device for secure

communication between the devices (fig. 2 element 221, 223, and 225). Moreover, Terao teaches wireless devices are securely communicated using common key to encrypt and decrypt data transmitted over the wireless communication system (page 3 par. 0063). In addition, Johnston teaches a method of distributing enciphering key to be used in encrypting and decrypting data at first and second wireless phones so as to provide secure data transmission between the two wireless phones in a wireless network (col. 2 lines 66-col. 3 lines 31).

Regarding argument (b), examiner disagrees with applicant. Based on the arguments set forth by the examiner for argument (a), the dependent claims stand rejected.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. Therefore, the examiner asserts that the system of the prior art, Johnston, Terao, and Ellison do teach or suggest the subject matter as recited in independent claims 1 and 13. Dependent claims 2-12, and 14-20 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action dated August 4, 2005. Accordingly, rejections for claims 1-20 are respectfully maintained.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1-3, 6-10, 12-15, and 17-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Johnston (U.S. Patent No.: 6,373,946 B1) in view of Terao et al. (Terao, Pub. No.: US 2001/0005682 A1), and in further view of Ellison (U.S. Patent Number: 6,073237)

As per claim 1, Johnston teaches a method of providing secure communications (Johnston Col. 3 lines 1-13) between a first wireless unit (Johnston Fig. 1 No. 2a) and a second wireless unit (Johnston Fig. 1 No. 2b), said method comprising the step of:

a first wireless unit (Johnston Fig. 1 No. 2a) and for use in secure communications (Johnston Col. 3 lines 1-13) over at least one wireless communications system (Johnston Col. 3 lines 43-59) between said first wireless unit (Johnston Fig. 1 No. 2a) and said second wireless unit (Johnston Fig. 1 No. 2b)

Johnston does not teach a first wireless unit and a second wireless unit having a common key.

However Terao discloses a wireless communication device (mobile phone) having a common key stored in the memory (Terao Page 18 claim 21).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Terao with in the system of Johnston because it would allow to encrypt transmission data and decrypt reception data (Terao Page 18 claim 21) in a wireless communication system.

Johnston and Terao do not explicitly teach providing common keys value to a first and second wireless unit.

However Ellison teaches sending or providing a common key to the user (Ellison Col. 10 claim 18)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Ellison with in the combination system of Johnston and Terao because it would allow to provide enhanced security and limit the ability of an active eavesdropper to access information by encrypting common key when passing it to the users or wireless phone users (Ellison Col. 3 lines 27-47).

As per claim 13, Johnston teaches a method of providing secure communications (Johnston Col. 3 lines 1-13) between a first wireless unit (Johnston Fig. 1 No. 2a) and a second wireless unit (Johnston Fig. 1 No. 2a), said method comprising the step of:

a first wireless unit (Johnston Fig. 1 No. 2a) from at least one wireless communications system (Johnston Col. 3 lines 43-59) for use in secure communications (Johnston Col. 3 lines 1-13) over at least one wireless communications system between said first wireless unit (Johnston Fig. 1 No. 2a) and said second wireless unit (Johnston Fig. 1 No. 2b).

Johnston does not teach a first wireless unit and a second wireless unit having a common key.

However Terao discloses a wireless communication device (mobile phone) having a common key stored in the memory (Terao Page 18 claim 21).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Terao with in the system of Johnston because

it would allow to encrypt transmission data and decrypt reception data (Terao Page 18 claim 21) in a wireless communication system.

Johnston and Terao do not explicitly teach receiving common keys value by a first wireless unit.

However Ellison teaches receiving a common key by the user (Ellison Col. 10 claim 18)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Ellison with in the combination system of Johnston and Terao because it would allow to provide enhanced security and limit the ability of an active eavesdropper to access information by encrypting common key when passing it to the users or wireless phone users (Ellison Col. 3 lines 27-47).

As per claim 2, Johnston, Terao, and Ellison teach all the subject matter as described above. In addition, Ellison teaches the method wherein said step of providing comprising the steps of:

generating a first key value corresponding to said first wireless unit (Ellison Fig. 1 No. 119);

generating a common key value (Ellison Col. 5 lines 1-6); and

sending said common key value to said first wireless unit using said first key value (Ellison Col. 10 claim 18). The rational for combining are the same as claim 1 above.

As per claim 3, Johnston, Terao, and Ellison teach all the subject matter as described above. In addition, Ellison teaches the method comprising the steps of:

generating a second key value corresponding to said second wireless unit (Ellison Fig. 1 No. 119; it is obvious to have the generation of the second key value corresponding to said second wireless unit because, in claim 2 above, the first wireless unit generates a common key corresponding to said second wireless unit); and

sending said common key value to said second wireless unit using said second key value (Ellison Col. 10 claim 18; it is obvious to send said common key value to said second wireless unit using said second key value because, in claim 2 above, said common key value is sent to said first wireless unit using said first key value). The rational for combining are the same as claim 1 above.

As per claim 6, Johnston, Terao, and Ellison teach all the subject matter as described above. In addition, Ellison teaches the method wherein said step of providing comprises the steps of:

encrypting said common key using said first key value (Ellison Col. 10 claim 18); and

transmitting said conmen key encrypted with said first key value to said first wireless unit (Ellison Col. 10 claim 18). The rational for combining are the same bases as claim 1 above.

As per claim 7, Johnston, Terao, and Ellison teach all the subject matter as described above. In addition, Ellison teaches the method wherein said step of providing comprises the steps of:

encrypting said common key with said second key value (Ellison Col. 10 claim 18); and

transmitting said common key encrypted with said second key value to said

second wireless unit (Ellison Col. 10 claim 18). The rational for combining are the same bases as claim 1 above.

As per claim 8, Johnston, Terao, and Ellison teach all the subject matter as described above. In addition, Ellison teaches the method wherein said step of generating said common key value comprises the steps of:

generating said common key as a function of at least one of said first key value and said second key value (Ellison Col. 5 lines 1-6, Fig. 1 No. 129). The rational for combining are the same as claim 1 above.

As per claim 9, Johnston, Terao, and Ellison teach all the subject matter as described above. In addition, Ellison teaches the method comprising the step of:

generating said common key as an encryption key (Ellison Col. 5 lines 1-6, Col. 10 claim 18). The rational for combining are the same as claim 1 above.

As per claim 10, Johnston, Terao, and Ellison teach all the subject matter as described above. In addition, Ellison teaches the method comprising the step of:

generating said common key as a session key (Ellison Col. 10 lines 18). The rational for combining are the same as claim 1 above.

As per claim 12, Johnston, Terao, and Ellison teach all the subject matter as described above. In addition, Terao teaches the method comprising the steps of:

mutually producing said common key by a first wireless communications system for said first wireless communications system and a second wireless communications system for said second wireless unit (Terao Col. 18 claim 21). The rational for combining are the same as claim 1 above.

As per claim 14, Johnston, Terao, and Ellison teach all the subject matter as described above. In addition, Ellison teaches the method comprising the steps of:

generating a first key value corresponding to said first wireless unit (Ellison Fig. 1 No. 119); and

obtaining said common key value by said first wireless unit using said first key value (Ellison Col. 10 claim 18). The rational for combining are the same as claim 1 above.

As per claim 15, Johnston, Terao, and Ellison teach all the subject matter as described above. In addition, Ellison teaches the method comprising the steps of:

generating a second key value corresponding to said second wireless unit (Ellison Fig. 1 No. 119; it is obvious to have the generation of the second key value corresponding to said second wireless unit because, in claim 2 above, the first wireless unit generates a common key corresponding to said second wireless unit); and

obtaining said common key value by said second wireless unit using said second key value (Ellison Col. 10 claim 18; it is obvious to obtain said common key value to said second wireless unit using said second key value because, in claim 2 above, said common key value is

sent to said first wireless unit using said first key value and obtained). The rational for combining are the same as claim 1 above.

As per claim 17, Johnston, Terao, and Ellison teach all the subject matter as described above. In addition, Ellison teaches the method wherein said step of providing comprises the steps of:

decrypting said common key using said first key value (Ellison Col. 9 claim 12). The rational for combining are the same as claim 1 above.

As per claim 18, Johnston, Terao, and Ellison teach all the subject matter as described above. In addition, Ellison teaches the method comprising the step of:

receiving said common key as an encryption key (Ellison Col. 10 claim 18). The rational for combining are the same as claim 1 above.

As per claim 19, Johnston, Terao, and Ellison teach all the subject matter as described above. In addition, Ellison teaches the method comprising the step of:

receiving said common key as a session key (Ellison Col. 10 claim 18, Col. 4 lines 18-35). The rational for combining are the same as claim 1 above.

5. Claims 4, 5, 11, 16 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Johnston (U.S. Patent No.: 6,373,946 B1), in view of Terao et al. (Terao, Pub. No.: US 2001/0005682 A1), and Ellison (U.S. Patent Number: 6,073237), and in further view of Berenzweig (U.S. Patent No. 6,584,310 B1).

As per claim 4, Johnston, Terao, and Ellison teach all the subject matter as described above.

Johnston, Terao, and Ellison do not explicitly teach said step of generating comprising the step of:

generating said first key value as a function of a first root key known only at said first wireless unit and a home wireless communications system for said first wireless unit.

However Berenzweig teaches generating said first key value as a function of a first root key (Berenzweig Col. 2 lines 20-41) known only at said first wireless unit and a home wireless communications system for said first wireless unit (Berenzweig Col. 2 lines 50-65).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Berenzweig with in the combination system of Johnston, Terao, and Ellison because it would allow to create a secure wireless communications by generating a session key and random number from a root key and pass random number to mobile terminal, and the user identification module receives the random number and utilizes the root key and random number and the algorithm calculates a signed response (Berenzweig Col. 2 lines 21-41).

As per claim 5, Johnston, Terao, Ellison, and Berenzweig teach all the subject matter as described above. In addition, Berenzweig teaches the method wherein said step of generating comprises the step of:

generating said second key value as a function of a second root key (Berenzweig Col. 2 lines 20-41) known only at said second wireless unit and at a home wireless communications system for said second wireless unit (Berenzweig Col. 2 lines 50-65; it is obvious to generate said second key value as a function of a second root key known only at said second wireless unit and at a home wireless communications system for said second wireless unit because, claim 4 above, generates said first key value as a function of a first root key known only at said first wireless unit and a home wireless communications system for said first wireless unit). The rational for combining are the same as claim 4 above.

As per claim 11, Johnston, Terao, and Ellison teach all the subject matter as described above.

In addition, Ellison teaches generating said common key as a session encryption key being a function of at least said first session key value (Ellison Col. 10 claim 18, Col. 4 lines 18-35);

Berenzweig teaches generating a first session key value (Berenzweig col. 2 lines 21-41) as a function of a first root key known only at said first wireless unit and a home wireless communications system for said first wireless unit (Berenzweig Col. 2 lines 42-65) The rational for combining are the same as claim 4 above.

As per claim 16, Johnston, Terao, Ellison, and Berenzweig teach all the subject matter as described above. In addition, Berenzweig teaches the method wherein said step of generating comprises the step of:

generating said first key value as a function of a first root key (Berenzweig Col. 2 lines 21-41)known only at said first wireless unit and a home wireless communications system for said first wireless unit (Berenzweig Col. 2 lines 51-65). The rational for combining are the same as claim 4 above.

As per claim 20, Johnston, Terao, Ellison, and Berenzweig teach all the subject matter as described above.

In addition, Ellison teaches receiving said common key as a session encryption key being a function of at least said first session key value (Ellison Col. 10 claim 18, col. 4 lines 18-35); and

Berenzweig teaches generating a first session key value (Berenzweig Col. 2 lines 21-41) as a function of a first root key known only at said first wireless unit and a home wireless communications system for said first wireless unit (Berenzweig Col. 2 lines 42-65). The rational for combining are the same as claim 4 above.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
August 4, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100